METHOD FOR ENABLING A NETWORK-ADDRESSABLE DEVICE TO DETECT USE OF ITS IDENTITY BY A SPOOFER

ABSTRACT

A defense against spoofing vandals is provided, where the defense enlists the network-addressable device whose identity is used by the vandal. A network-addressable device checks incoming messages for communication protocol violations that indicate that a spoofer is using the identity of the network-addressable device. When such a protocol violation is detected, the network-addressable device records attributes of the incoming message in a spoofing logbook database. Further, the network-addressable device increments a counter associated with the identity of the spoofer's target. The value of the counter is compared with a predetermined threshold, in order to determine if the supposed spoofing is an isolated incident or part of a persistent attack. When the value of the counter exceeds the threshold, the network-addressable device constructs a spoofing alert, and sends the spoofing alert to a network administrator. The network-addressable device then rejects the message associated with the protocol violation.